IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

Scott Thomas ELLIOTT, et al.	Confirmation No. 3264
Serial No: 09/957,415	Group Art Unit: 2131
Filed: September 20, 2001	Examiner: Chai, Longbit

For: METHOD AND SYSTEM FOR KEY USAGE CONTROL IN AN EMBEDED SECURITY SYSTEM

APPEAL BRIEF

Janyce R. Mitchell
Attorney for Appellants
Lenovo
Sawyer Law Group LLP

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

Scott Thomas ELLIOTT, et al.	Confirmation No. 3264
Serial No: 09/957,415	Group Art Unit: 2131
Filed: September 20, 2001	Examiner: Chai, Longbit

For: METHOD AND SYSTEM FOR KEY USAGE CONTROL IN AN EMBEDED SECURITY SYSTEM

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. § 1.193(b)(1) as follows:

I. REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to Lenovo.

II. RELATED APPEALS AND INTERFERENCES

Appellant states that, upon information and belief, Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-22 are pending. Application Serial No. 09/957,413 (the instant application) as originally filed included claims 1-19. In response to an Office Action dated February 11, 2005, claims 20-22 were added. In response to a Final Office Action dated May 26, 2005, claims 30-22 were amended to correct a spelling error. Claims 1-22 are on appeal and all applied prospective rejections concerning claims 1-22 are herein being appealed.

IV. STATUS OF AMENDMENT

The Examiner indicated in the Advisory Action dated August 24, 2005, that the amendment to the claims in response to the Final Office Action would be entered in response to the filing of the Notice of Appeal.

V. SUMMARY OF THE INVENTION

The present invention provides a method and system for control of key pair usage in a computer system. Key pair material for utilization with an embedded security chip of the computer system is created. Specification, page 4, lines 10-12. The key pair material includes tag data. Specification, page 4, line 12. It is determined whether the key pair material is bound to the embedded security chip based on the tag data. Specification, page 4, lines 12-14. Through the present invention, more flexibility for control over which keys are bound to an embedded security system is achieved. Specification, page 4, lines 15-16.

Figure 1 depicts an embedded security chip coupled to a main processor. Specificatoin, page 1, lines 17-18. In general, cryptographic operations are routed through the embedded security chip (by cryptographic middleware), which enables applications using appropriate APIs to secure cryptographic operations through the built-in hardware to offer more security than with a software solution. Specification, page 1, line 20-page 2, line 3.

The embedded security chip, such as that disclosed in Figure 1, employs a hierarchical key structure to manage keys. Each level is secured through the level below it by encrypting that level's private key with the public key of the underlying level's key pair. Specification, page 2, line 20-page 3, line 2. Thus, for a four level structure, level 3's private key is encrypted with the public key of level 2, level 2's private key is encrypted with the public key of level 1, and so on. As originally defined, a Level 0 or base hardware key pair resides entirely on the embedded security chip. Specification, page 3, lines 4-5. The hardware key pair is unique to the system. Rights and ownership of the hardware private key are established through an administrator password. Specification, page 3, lines 6-10

In contrast, Figure 2A illustrates a data structure 100 for allowing for managing the binding of the key pair to the security chip. Specification, page 5, lines 22-page 6, line 1. The data structure includes key pair material and an associated tag, which can be used to determine whether the key pair material is to be bound to the security chip. Specification, page 6, lines 2-3. For example, Figure 2B illustrates an example of a hierarchical key pair structure employing tag data to indicate binding. In the embodiment shown, there are four levels: a hardware key pair (level 0, item 201), the platform key pair (level 1, item 202), key encrypting key pairs (level 2, items 220 and 220'), and user key pairs (level 3, items 240-244 and 240'-246'). Specification, page 6, lines 4-8. Depending upon whether the tag is set of the key pair, it can be determined whether binding of these key pairs , and whether the keys are available to the user based on the binding. Specification, page 6, lines 8-13.

Figure 3 depicts a flow chart of a process for key usage control in accordance with the present invention. Specification, page 6, lines 15-17. The key pair is created, preferably in a standard manner except that tag data is associated with the key pair. Specification, page 6, lines 16-19. The combination of the key pair and tag data are provided to the embedded security chip. Specification, page 6, lines 20-21. The status of the tab for the key pair is checked by the embedded security chip. Specification, page 6, lines 21-23. If the tag indicates that the key is a binding-required key, the embedded security chip only allows cryptographic functions to be performed using this key. Specification, page 6, line 21-page 7, line 1. Otherwise, the embedded security chip may allow all operations on the embedded security chip with that key regardless of binding, under the assumption that the user is verified by their password. Specification, page 7, lines 1-4.

Thus, the inclusion of tag data in the key material allows user keys to be designated as not binding-required, so that they may be verified securely on any system. Access to the embedded security subsystem remains secure because the platform is verified only on the system where binding is established. In this manner, there is more selective allowance of key types based on binding. Specification, page 7, lines 9-14.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) whether claims 1-23 are each unpatentable under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,792,113 (Ansell) in view of U.S. Patent Publication No. 2002/0071559 (Christensen).

VII. ARGUMENTS

A. Summary of the Applied Rejections

In the Final Office Action, dated May 26, 2005, the Examiner rejected claims 1-22 under 35 U.S.C. § 103 as being unpatentable over Ansell in view of Christensen. In so doing, the Examiner indicated that Ansell teaches that a security key pair can be associated with either machine binding (bound) or user-binding (not bound). Thus, the Examiner cited col. 2, lines 33-64; col. 10, lines 10-25; and elements 140, 2404 and 308 of Figure 3B. The Examiner indicated that Ansell does not expressly disclose creating key pair material for use with an embedded security chip of a computer system. Consequently, the Examiner relied upon Christensen, paragraphs 245 and 252 for this teaching. Further, in response to Appellant's arguments, the Examiner stated that "the collection of security key passport data structures combining with user option indicator is equivalent to the key material including tag data to meet the claim language." With respect to claims 20-22, the Examienr cited Figures 3A and 3B of Ansell as depicting a hierarchical structure.

B. The Cited Prior Art

Ansell describes a system used to protect content of digital storage media unauthorized copying while allowing unimpeded use of the content by the owner. Ansell, col. 2, lines 21-25. To do so, Ansell describes a system that allows for conversion between binding to a machine and binding to a user by employing keys rather than modifying the content itself. Ansell, col. 2, lines 28-34. For machine binding, Ansell describes creating a passport that contains the private key for the machine and a public key for the machine. Ansell, col. 2, lines 35-38. The private key is based on a hardware identifier for the machine. Ansell, col. 2, lines 38-40. This hardware identifier is specific to a hardware device, for example a hash of the MAC address for the computer. Ansell, col. 6, lines 5-18. The public key is the reciprocal of the private key and, therefore, the reciprocal of the hardware identifier of the machine. Ansell, col. 2, lines 35-38. Ansell also allows the creation of a passport for user binding. Such a passport also includes a private key and a public key that is the reciprocal of the private key. Ansell, col. 2, lines 54-64. User binding, the private key is based upon a password provided by the user. Ansell, col. 2, lines 56-60. The public in the user-bound case is, therefore, the reciprocal of the password. Ansell also states that the user must select *either* the machine bound password or the user-bound password. Ansell, col. 3, lines 10-11.

Ansell indicates that user binding is less limiting than machine binding. Ansell, col. 3, lines 17-18. Consequently, Ansell discloses changing, or "upgrading" the passport from machine binding to a passport for user binding. However, in order to do so, Ansell describes creating a *new* user passport using the keys of the machine-bound passport in conjunction with the user's password. Ansell, col. 3, lines 25-46. In particular, Ansell states:

> [a] machine-bound passport can be upgraded to a user-bound passport without modifying the bound content. In particular, the original private and public keys of the machine-bound passport are used in a ***newly created*** user-passport such that re-encryption of the content is not required. Specifically, the private key of the machine-bound passport, in cleartext form, is included in the user-bound passport and encrypted using a user-supplied password to bind the private key to the user. In addition, private user information is collected and verified and included in the user-bound passport. Thus, the user-supplied password decrypts the private key to provide the same cleartext private key that results from decrypting the private key of the machine-bound passport using the hardware identifier. Accordingly, the previously machine-bound content can now be decrypted using the user-bound passport.

Ansell, col. 3, lines 25-33.

Christenson describes a system for decrypting content, such as copyrighted content utilizing keys. Christensen, Abstract and col. 1, lines 1-4. In order to do so, Christensen describes using keys. Christensen, paragraph 245. In one embodiment, Christensen describes using "a hardware processor containing an inaccessible part." Christensen, paragraph 244. Christensen further describes storing portions of the key in the inaccessible part of the hardware processor. Christensen, paragraph 245. Christensen further states that the hardware processor may be a "silicon chip of the kind which is often used in computer devices. . . [or for example] a device, e.g. a smart card, which may be incorporated into other pieces of hardware, e.g. output devices such as printers, screens, etc." Christensen, paragraph 252.

C. Claims 1-22 Are Not Unpatentable Under 35 U.S.C. § 103.

Appellant respectfully submits that the applied rejections of claims 1, 7, and 16 under 35 U.S.C. § 103 are without merit as the Examiner has completely failed to explain why Ansell in view of Christensen teaches or suggests the method, system, and computer-readable medium recited in independent claims 1, 7 and 16.

Claim 1 recites a method for control of key pair usage in a computer system. The method recited in claim 1 includes creating key pair material for utilization with an embedded security chip of the computer system, wherein the key pair material includes tag data. Claim 1 further recites determining whether the key pair material is bound to the embedded security chip based on the tag data. Claim 7 recites an analogous computer system including a main processor and a security processor. The security processor stores tag data with key pair material and determines binding of the key pair material to the security processor based on the tag data. Similarly, claim 16 recites a method for controlling usage of key pairs in a hierarchical structure of key pairs in an embedded security chip. Claim 16 recites storing tag data with key pair data for each level of the hierarchical structure and determining whether the key pair data is bound to the embedded security chip based on the tag data.

Thus, claims 1, 7, and 16 utilize tag data of the key pair material in order to determine the binding status of the key pair. Consequently, a user can either be bound to a particular system or may be verified securely on any system. Specification, page 7, lines 9-13.

Ansell in view of Christensen fail to teach or suggest the methods and system recited in claims 1, 7, and 16. In particular, Ansell in view of Christensen fails to teach or suggest utilizing key pair material for use with an embedded security chip, or security processor, in conjunction with determining binding of the key pair material to the embedded security chip/security processor based on the tag data.

As discussed above, Ansell does describe the use of keys and passports. However, Ansell expressly states that a user selects *either* a machine bound or a user bound passport. Further, Ansell describes the *conversion* of a machine bound passport to a user bound passport. Ansell also describes the use of different information for keys are used for a machine bound passport and a user passport. In particular, a hardware identifier is used for the creation of keys in a machine-bound passport and a user-selected password is used for the creation of keys in the user bound passport. Consequently, Ansell does not utilize tags in conjunction with key pair material. Moreover, Ansell does not utilize keys in order to determine the binding of the key pair material. Instead, different passports are used.

Christensen fails to remedy the defects of Ansell. Christensen does describe the use of keys. However, Appellant has found no mention in Christensen of user binding and machine binding, much less of using tags to determine whether the keys are user bound or machine bound. Both Ansell and Christensen thus fail to teach or suggest the use of tag data to determine whether keys are bound to an embedded security processor/security chip. Consequently, any combination of

Ansell and Christensen fail to teach or suggest such a feature. Ansell in view of Christensen, therefore, fail to teach or suggest the methods and system recited in claims 1, 7, and 16.

Further, Ansell in view of Christensen fails to teach or suggest the use of an embedded security chip or processor. The Examiner has acknowledged that Ansell fails to disclose creating key pair material for utilization with an embedded security chip of the computer system. Consequently, the Examiner has relied upon paragraphs 245 and 252 of Christensen to teach the use of such an embedded security chip. However, the cited portions of Christensen merely describe providing a decryption key to a part of the processor or to an "inaccessible" part of the processor. Christensen further describes the processor as being a silicon chip or other device such as a Smart Card that can be incorporated into the other pieces of hardware. In contrast, the specification specifically defines the embedded security processor/security chip as a separate "cryptographic microprocessor" that is embedded in the system board of the computer system and through which security operations are routed. Specification, page 1, lines 14-16, page 1 and line 18-page 2, line 4. Such an embedded security processor is, therefore, a separate processor embedded in the system board, not merely an "inaccessible portion" of a processor nor a removable device such as a Smart Card. Consequently, the recited embedded security processor/security chip is distinct from the inaccessible portion of the processor described by Christensen. Moreover, with respect to claim 7, Appellant notes that separate main and security processor are recited. This is also distinct from the inaccessible portion of the processor or other hardware device described by Christensen. As a result, Ansell in view of Christensen neither teach nor suggest the use of the recited embedded security processor/security chip. Ansell in view of Christensen do not, therefore, teach or suggest the methods and system recited in claims 1, 7, and 16. Consequently, Appellant respectfully submits that claims 1, 7, and 16 are allowable over the cited references.

Moreover, claim 16 recites storing tag data along with key material in conjunction with using the tag data to determine whether the key material is bound to the system. This feature is neither taught nor suggested by Ansell in view of Christensen. Ansell describes changing a machine-bound passport to a user-bound passport. However, the history of the keys, including the whether the key/passport has been converted from bound to unbound is stored not in the passport, but in a table in a certificate database. Ansell, col. 10, line 6-64. Appellant respectfully submits, therefore, that data relating to the nature (bound/unbound) of the key resides in the certificate database. Consequently, Ansell does not store information relating to the binding of the key pair with the key in the passport, but in the separate certificate database. Thus, Ansell fails to teach or suggest storing tag information from which the binding state of the key material can be determined along with the key material. Christensen fails to remedy this defect. As discussed above, Appellant has found no mention in the cited portions of Christensen of storing tags with the key material, or that such tags can be used to determine whether the key material is bound. Consequently, any combination of Ansell and Christensen would also fail to include such a feature.

Consequently, Ansell in view of Christensen fail to teach or suggest storing tag data that determines whether the key material is bound along with key material. Ansell in view of Christensen thus fail to teach or suggest the methods and system recited in claims 1, 7, and 16. Accordingly, for the above-identified reasons, Appellant respectfully submits that claims 1, 7, and 16 are allowable over the cited references.

Claims 2-6 and 20 depend upon independent claim 1. Claims 8-15 and 21 depend upon independent claim 7. Consequently, the arguments herein with respect to claims 1 and 7 apply with full force to claims 2-6, 8-15 and 20-21. Claims 17-19 and 22 depend upon claim 16.

Consequently, the arguments herein with respect to claim 16 apply with full force to claims 17-19 and 22. Accordingly, Appellant respectfully submits that claims 2-6, 8-15, and 17-22 are allowable over the cited references.

Furthermore, Appellant respectfully submits that claims 20-22 are separately allowable over the cited references. Claims 20-22 recite that the key pair materials are created or the hierarchical structure is organized such that key pair material for a portion of "each of at least two of the different levels are not bound." Appellant has found no mention in Ansell or Christensen of organizing the hierarchy or creating the key pair material such that key pair material for a portion of each of at least two of the different levels is not bound. Ansell in view of Christensen thus fail to teach or suggest the method and systems of claims 20-22. Accordingly, Appellant respectfully submits that claims 20-22 are separately allowable over the cited references.

Accordingly Appellant respectfully requests that the Board reverse the final rejection of claims 1-22 under 35 U.S.C. § 103.

D. Summary of Arguments

For all the foregoing reasons, it is respectfully submitted that claims 1-22 (all the claims presently in the application) are patentable for defining subject matter which would not have been obvious under 35 U.S.C. § 103. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" section is contained on separate sheets following the signatory portion of this Appeal Brief.

Authorization for payment of the required Brief fee is contained in the transmittal letter for this Brief. Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 50-3533 (Lenovo).

Very truly yours,

November 21, 2005

*/Janyce R. Mitchell/*Reg. No. 40,095
Janyce R. Mitchell
Attorney for Appellants
Reg. No. 40,095
(650) 493-4540

VIII. CLAIMS APPENDIX

1. A method for control of key pair usage in a computer system, the method comprising:

(a) creating key pair material for utilization with an embedded security chip of the computer system, the key pair material including tag data; and

(b) determining whether the key pair material is bound to the embedded security chip based on the tag data.

2. The method of claim 1 wherein the tag data further comprises a bit to indicate whether binding is required for the key pair material.

3. The method of claim 1 wherein creating key pair material further comprises creating key pair material of different levels.

4. The method of claim 3 wherein the different levels further comprise four levels.

5. The method of claim 4 wherein the four levels further comprise a hardware key pair level, a platform key pair level, a user key pair level, and a credential key pair level.

6. The method of claim 5 wherein including tag data further comprises including a tag for indicating binding is required for the platform key pair level.

7. A computer system with control over key pair usage, the computer system comprising:

a main processor for controlling the computer system; and

a security processor coupled to the main processor for embedded security in the computer system, the security processor for storing tag data with key pair material and determining binding of the key pair material to the security processor based on the tag data.

8. The system of claim 7 further comprising means for security setup to provide an interface on the computer system for administration of the security processor, including providing the tag data.

9. The system of claim 8 wherein the tag data comprises a bit to indicate whether binding is required for the key pair material.

10. The system of claim 7 wherein the security processor includes memory for storing the key pair material.

11. The system of claim 7 wherein the security processor manages the key pair material in a hierarchical structure.

12. The system of claim 11 wherein the hierarchical structure further comprises a four level structure.

13. The system of claim 12 wherein the four level structure further comprise a hardware key pair level, a platform key pair level, a user key pair level, and a credential key pair level.

14. The system of claim 13 wherein the key pair material further comprises a tag to indicate binding is required for the platform key pair level.

15. The system of claim 14 wherein the key pair material further comprises a tag to indicate binding is not required for the user key pair level.

16. A method for controlling usage of key pairs in a hierarchical structure of key pairs in an embedded security chip, the method comprising:

storing tag data with key pair data for each level of the hierarchical structure; and

determining whether the key pair data is bound to the embedded security chip based on the tag data.

17. The method of claim 16 wherein storing tag data further comprises storing a set tag bit to indicate that binding is required and storing a reset tag bit to indicate that no binding is required.

18. The method of claim 17 further comprising utilizing the reset tag bit with a user key pair level in the hierarchical structure to allow user key pairs to be verified securely on more than one computer system.

19. The method of claim 18 further comprising utilizing the set tag bit with a platform key pair level in the hierarchical structure to allow a platform key pair to be verified only on a computer system where binding with the embedded security chip is established.

20. The method of claim 3 wherein creating key pair material further comprises creating key pair material of the different levels such that key pair material for a portion of each of at least two of the different levels are not bound.

21. The system of claim 11 wherein the hierarchical structure is organized such that key pair material for portion of each of at least two levels of the hierarchical structure are not bound.

22. The system of claim 16 wherein the hierarchical structure is organized such that key pair material for portion of each of at least two levels of the hierarchical structure are not bound.

IX. EVIDENCE APPENDIX

X. RELATED PROCEEDINGS APPENDIX

AF/2131/
IFW

TRANSMITTAL FORM

Attorney Docket No.
RPS920010044US1/2145P

In re the application of: **Scott T. ELLIOTT, et al.**

Confirmation No: **3264**

Serial No: **09/957,415**

Group Art Unit: **2131**

Filed: **September 20, 2001**

Examiner: **Chai, Longbit**

For: **Method and System for Key Usage Control in an Embedded Security System**

ENCLOSURES ***(check all that apply)***

□ Amendment/Reply	□ Assignment and Recordation Cover Sheet	□ After Allowance Communication to Group
□ After Final	□ Part B-Issue Fee Transmittal	□ Notice of Appeal
□ Information disclosure statement	□ Letter to Draftsman	☒ Appeal Brief
□ Form 1449	□ Drawings	□ Status Letter
□ (X) Copies of References	□ Petition	☒ Postcard
□ Extension of Time Request *	□ Fee Address Indication Form	□ Other Enclosure(s) *(please identify below):*
□ Express Abandonment	□ Terminal Disclaimer	
□ Certified Copy of Priority Doc	□ Power of Attorney and Revocation of Prior Powers	
□ Response to Incomplete Appln	□ Change of Correspondence Address	
□ Response to Missing Parts	*Extension of Term: Pursuant to 37 CFR 1.136, Applicant petitions the Commissioner to extend the time for response for xxxxxx month(s), from to .	
□ Executed Declaration by Inventor(s)		

CLAIMS

FOR	Claims Remaining After Amendment	Highest # of Claims Previously Paid For	Extra Claims	RATE	FEE
Total Claims	0	0	0	$ 50.00	$ 0.00
Independent Claims	0	0	0	$200.00	$ 0.00
				Total Fees	$ 0.00

METHOD OF PAYMENT

□ Check no. _____ in the amount of $ _________ is enclosed for payment of fees.

☒ Charge $ 500.00 to Deposit Account No. 50-3533 (Lenovo) for payment of Appeal Brief filing fees.

☒ Charge any additional fees or credit any overpayment to Deposit Account No. 50-3533 (Lenovo)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Attorney Name	Janyce R. Mitchell, Reg. No. 40,095
Signature	/*Janyce R. Mitchell*/Reg. No. 40,095 Janyce R. Mitchell
Date	November 21, 2005

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 21, 2005

Type or printed name	Jackie Tanda
Signature	Jackie Tanda